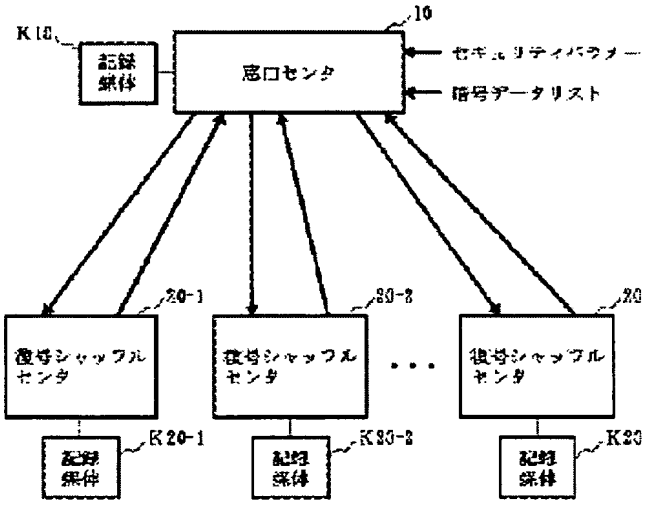
ANONYMOUS DECODING SYSTEM, ANONYMOUS DECODING METHOD, AND PROGRAM THEREFOR

Publication number: JP2002237810
Publication date: 2002-08-23
Inventor: SAKO KAZUE; MORI KENGO
Applicant: NIPPON ELECTRIC CO
Classification:
- international: ***H04L9/30; H04L9/32;*** **H04L9/28; H04L9/32;** (IPC1-7): H04L9/08; G06F17/60
- european: H04L9/30; H04L9/32S
Application number: JP20010035030 20010213
Priority number(s): JP20010035030 20010213

Also published as:
EP1361693 (A1)
WO02065695 (A1)
US2004114763 (A
CA2441496 (A1)

Abstract of **JP2002237810**

PROBLEM TO BE SOLVED: To enable an anonymous decoding system to be easily controlled and its initial setting operation to be surely and easily carried out. SOLUTION: A window center 10 sends security parameters and common public information formed on the basis of the security parameters to decoding shuffle centers 20-1 to 20-m, and the decoding shuffle centers 20-1 to 20-m produce public keys and decoding keys and send back the public keys to the window center 10. The window center 10 synthesizes the received public keys, produces and publicizes encrypting public keys. The window center 10 transfers the encrypted data list to the decoding the j-th shuffle center 20-j when an encrypted data list is decoded, then the window center 10 changes a processing sequence and transfers the received partially decoded data list to the decoding shuffle center 20-(j+1), and the above process is repeatedly carried out. These processes are carried out until the data list is transferred to the last decoding shuffle center 20-m, and the data list sent from the decoding shuffle center 20-m is made to serve as a decoding result.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－237810
（P2002－237810A）
(43)公開日　平成14年８月23日(2002.8.23)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　17/60	１４８	５Ｊ１０４
Ｇ０６Ｆ　17/60	１４８		５１２	
	５１２	Ｈ０４Ｌ　9/00	６０１Ｃ	
			６０１Ｆ	

審査請求　未請求　請求項の数68　ＯＬ　（全 18 頁）

(21)出願番号　特願2001－35030(P2001－35030)

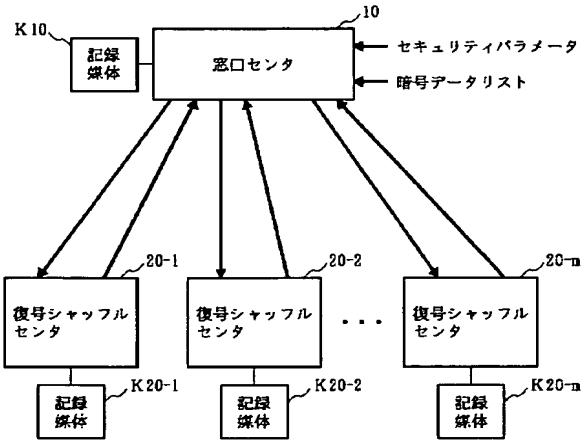
(22)出願日　平成13年２月13日(2001.2.13)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　森　健吾
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088959
弁理士　境　廣巳

Ｆターム(参考)　5J104 AA16 EA04 EA24 JA21 PA17

(54)【発明の名称】　匿名復号システム及び匿名復号方法並びにプログラム

(57)【要約】
【課題】　匿名復号システムの管理を容易にすると共に、初期設定操作を容易且つ確実に行えるようにする。
【解決手段】　窓口センタ10は、セキュリティパラメータとそれに基づいて生成した共通公開情報を各復号シャッフルセンタ20-1～20-mへ送り、各復号シャッフルセンタ20-1～20-mは、公開鍵，復号鍵を生成し、公開鍵を窓口センタ10へ返送する。窓口センタ10は、返送された各公開鍵を合成して暗号化用公開鍵を生成し、公開する。また、窓口センタ10は、暗号データリストの復号時、処理順序が第ｊ番目の復号シャッフルセンタ20-jに暗号データリストを転送し、返送されてきた順番入れ替え，部分復号処理の済んだデータリストを次の復号シャッフルセンタ20-(j+1)へ転送するという処理を繰り返し行う。このような処理を最後の復号シャッフルセンタ20-mまで行い、そこから返送されたデータリストを復号結果とする。



1

【特許請求の範囲】

【請求項１】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムにおいて、

外部から暗号データリストが入力された場合、該暗号データリストを復号シャッフルセンタへ転送し、前記復号シャッフルセンタからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する窓口センタと、

該窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送する復号シャッフルセンタとを備えたことを特徴とする匿名復号システム。

【請求項２】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムにおいて、

暗号データリストを外部から受け取る窓口センタと、

それぞれが復号鍵を所有する複数の復号シャッフルセンタとから成立ち、

前記窓口センタは、受け取った暗号データリストを第１の復号シャッフルセンタに転送し、

前記第１の復号シャッフルセンタは、前記窓口センタから受け取った暗号データリストに対して、対応する公開情報を用いて順番入れ替え処理を行い、対応する復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタに返送し、

前記窓口センタは、前記第１の復号シャッフルセンタから返送されたデータリストを、第２の復号シャッフルセンタに送信し、

前記窓口センタは、最後の復号シャッフルセンタから返送されたデータリストを、復号結果リストとして出力することを特徴とする匿名復号システム。

【請求項３】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、該暗号データリスト上の各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムにおいて、

窓口センタと、それぞれが復号鍵を所有する複数の復号シャッフルセンタとを備え、

前記窓口センタが、

外部から暗号データリストが入力された場合、該暗号データリストを処理順序が第１番目の復号シャッフルセンタへ転送し、処理順序が最後の復号シャッフルセンタ以外の復号シャッフルセンタからデータリストが返送されてきた場合、処理順序が前記データリストの返送元復号シャッフルセンタの次の復号シャッフルセンタに対して前記返送されてきたデータリストを暗号データリストとして転送し、処理順序が最後の復号シャッフルセンタからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する構成を有し、

前記各復号シャッフルセンタが、

前記窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送する構成を有することを特徴とする匿名復号システム。

【請求項４】　請求項１，２または３記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記窓口センタに報告する構成を有することを特徴とする匿名復号システム。

【請求項５】　請求項１，２または３記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記処理結果のデータリストに付して前記窓口センタに報告する構成を有することを特徴とする匿名復号システム。

【請求項６】　請求項４または５記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証する構成を有することを特徴とする匿名復号システム。

【請求項７】　請求項４または５記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証した後、前記復号シャッフルセンタから返送されてきたデータリストを暗号データリストとして、処理順序が次の復号シャッフルセンタに転送する構成を有することを特徴とする匿名復号システム。

【請求項８】　請求項４，５，６または７記載の匿名復号システムにおいて、

前記窓口センタは、前記復号結果リストに、全復号シャッフルセンタから報告された証明を添付して出力する構成を有することを特徴とする匿名復号システム。

【請求項９】　請求項１，２または３記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行う構成を有することを特徴とする匿名復号システム。

【請求項１０】　請求項１，２または３記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信元のデジタル署名を付与する構成を有することを特徴とする匿名復号システム。

【請求項１１】　請求項１，２または３記載の匿名復号システムにおいて、

同一処理対象に対する、互いに関連する公開情報，暗号データリスト，復号シャッフルセンタが所有する復号鍵に共通のセッションＩＤを付与し、

前記窓口センタは、或るセッションＩＤに対応する暗号データリストを復号シャッフルセンタへ転送する場合および復号シャッフルセンタから返送されてきた或るセッションＩＤの付与されたデータリストを暗号データリストとして復号シャッフルセンタへ転送する場合、前記暗号データリストに前記或るセッションＩＤを付与して復号シャッフルセンタへ転送する構成を有し、

前記復号シャッフルセンタは、前記窓口センタから或るセッションＩＤの付与された暗号データリストが転送されてきた場合、前記或るセッションＩＤの付与されている公開情報を用いて順番入れ替え処理を行い、前記或るセッションＩＤの付与されている復号鍵を用いて部分復号を行い、その結果のデータリストに前記或るセッションＩＤを付与して前記窓口センタに返送する構成を有することを特徴とする匿名復号システム。

【請求項１２】　請求項１，２または３記載の匿名復号システムにおいて、

前記窓口センタが、

セキュリティパラメータが入力されたとき、該セキュリティパラメータに基づいて共通公開情報を作成し、該作成した共通公開情報を全復号シャッフルセンタへ通知し、全復号シャッフルセンタから公開鍵が返送されてきたとき、全復号シャッフルセンタからの公開鍵に基づいて暗号化用公開鍵を生成すると共に、該生成した暗号化用公開鍵と前記共通公開情報とを含んだ公開情報を公開する構成を有し、

前記復号シャッフルセンタが、

前記窓口センタから通知された共通公開情報に基づいて、公開鍵および復号鍵を生成し、前記生成した公開鍵を前記窓口センタへ返送する構成を有することを特徴とする匿名復号システム。

【請求項１３】　請求項１２記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、公開鍵を前記窓口センタへ返送するとき、正しく前記公開鍵を生成したことの証明を付して前記窓口センタに返送する構成を有することを特徴とする匿名復号システム。

【請求項１４】　請求項１３記載の匿名復号システムにおいて、

前記窓口センタは、公開鍵に付された証明が正しいことを検証する構成を有することを特徴とする匿名復号システム。

【請求項１５】　請求項１３または１４記載の匿名復号システムにおいて、

前記窓口センタは、公開鍵と、公開鍵に付与された証明を公開情報とともに公開する構成を有することを特徴とする匿名復号システム。

【請求項１６】　請求項１２記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行う構成を有することを特徴とする匿名復号システム。

【請求項１７】　請求項１２記載の匿名復号システムにおいて、

前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信者のデジタル署名を付与する構成を有することを特徴とする匿名復号システム。

【請求項１８】　請求項１１記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタに対して暗号データリストを転送する際、前記セッションＩＤに加えて、自窓口センタに付与されている窓口センタＩＤ，転送先の復号シャッフルセンタに付与されている復号シャッフルセンタＩＤ及び自窓口センタの署名も付加する構成を有することを特徴とする匿名復号システム。

【請求項１９】　請求項１１記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、前記セッションＩＤに加えて、自復号シャッフルセンタに付与されている復号シャッフルセンタＩＤ，前記窓口センタに付与されている窓口センタＩＤ及び自復号シャッフルセンタの署名も付加する構成を有することを特徴とする匿名復号システム。

【請求項２０】　請求項１９記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、正しく順番入れ替え処理を行ったことの証明データ及び正しく部分復号処理を行ったことの証明データも付加する構成を有することを特徴とする匿名復号システム。

【請求項２１】　請求項８記載の匿名復号システムにおいて、

前記窓口センタが出力する情報が、自窓口センタに付与されている窓口センタＩＤ，外部から入力した暗号データリスト，該暗号データリストに対する復号結果リスト，前記暗号データリストに付与されているセッションＩＤ，全復号シャッフルセンタから返送されてきた全データ及び窓口センタの署名を含むことを特徴とする匿名復号システム。

【請求項２２】　請求項１２記載の匿名復号システムにおいて、

前記窓口センタは、復号シャッフルセンタに対して共通

公開情報およびセキュリティパラメータを通知する際、自窓口センタに付与されている窓口センタＩＤ，復号を行う全復号シャッフルセンタの復号シャッフルセンタＩＤ，セッションＩＤ及び窓口センタの署名を付加する構成を有することを特徴とする匿名復号システム。

【請求項２３】　請求項１２または１３記載の匿名復号システムにおいて、復号シャッフルセンタは、窓口センタに返信する情報に、前記窓口センタに付与されている窓口センタＩＤ，セッションＩＤ，自復号シャッフルセンタの復号シャッフルセンタＩＤ及び自復号シャッフルセンタの署名を付加する構成を有することを特徴とする匿名復号システム。

【請求項２４】　請求項１２記載の匿名復号システムにおいて、

前記窓口センタが公開する公開情報は、自窓口センタに付与されている窓口センタＩＤ，セッションＩＤ，セキュリティパラメータ，暗号化用公開鍵，全復号シャッフルセンタの復号シャッフルセンタＩＤ及び全復号シャッフルセンタが生成した公開鍵を含むことを特徴とする匿名復号システム。

【請求項２５】　請求項４，５，９または１３記載の匿名復号システムにおいて、

復号シャッフルセンタが行った証明は、第三者により検証できるものであることを特徴とする匿名復号システム。

【請求項２６】　請求項１，２または３記載の匿名復号システムにおいて、前記復号シャッフルセンタは、順番入れ替え処理に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前計算したデータを用いて順番入れ替え処理を行う構成を有することを特徴とする匿名復号システム。

【請求項２７】　請求項５記載の匿名復号システムにおいて、

前記復号シャッフルセンタは、順番入れ替え処理が正しいことを証明する証明データの生成に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前に計算したデータを用いて前記証明データを生成する構成を有することを特徴とする匿名復号システム。

【請求項２８】　請求項１乃至２７記載の何れか１つの匿名復号システムにおいて、

各投票者から送られてくる、投票データを前記公開情報に基づいて暗号化した暗号化投票データを受け付け、その中から正当な投票者の正当な暗号化投票データを選別し、該選別した暗号化投票データを暗号データリストとして前記窓口センタに送信する投票管理センタを備えたことを特徴とする匿名復号システム。

【請求項２９】　請求項２８記載の匿名復号システムにおいて、

前記各投票者は、正しく投票データを暗号化したことを証明する証明データを前記投票管理センタへ送信し、

前記投票管理センタは、各投票者から送られてきた証明データを検証する構成を有することを特徴とする匿名復号システム。

【請求項３０】　請求項１乃至２７記載の何れか１つの匿名復号システムにおいて、

各入札者から送られてくる、入札値を前記公開情報に基づいて暗号化した暗号化入札値を受け付け、その中から正当な入札者の正当な暗号化入札値を選別し、該選別した暗号化入札値を暗号化データリストとして前記窓口センタへ送信する入札管理センタを備えたことを特徴とする匿名復号システム。

【請求項３１】　請求項３０記載の匿名復号システムにおいて、

前記各入札者は、正しく入札値を暗号化したことを証明する証明データを前記入札管理センタへ送信し、

前記入札管理センタは、各入札者から送られてきた証明データを検証する構成を有することを特徴とする匿名復号システム。

【請求項３２】　請求項１乃至請求項２７記載の何れか１つの匿名復号システムにおいて、

各アンケート回答者から送られてくる、アンケート回答を前記公開情報に基づいて暗号化した暗号化アンケート回答を受け付け、その中から正当なアンケート回答者の正当な暗号化アンケート回答を選別し、該選別した暗号化アンケート回答を暗号化データリストとして前記窓口センタへ送信する受付センタを備えたことを特徴とする匿名復号システム。

【請求項３３】　請求項３２記載の匿名復号システムにおいて、

前記アンケート回答者は、正しくアンケート回答を暗号化したことを証明する証明データを前記受付センタへ送信し、

前記受付センタは、各アンケート回答者から送られてきた証明データを検証する構成を有することを特徴とする匿名復号システム。

【請求項３４】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号方法において、

窓口センタが、外部から暗号データリストが入力された場合、該暗号データリストを復号シャッフルセンタへ転送し、

前記復号シャッフルセンタが、前記窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送し、

前記窓口センタが、前記復号シャッフルセンタからデー

タリストが返送されてきた場合、該データリストを復号結果リストとして出力することを特徴とする匿名復号方法。

【請求項３５】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号方法において、

窓口センタが、外部から受け取った暗号データリストを第１の復号シャッフルセンタに転送し、

前記第１の復号シャッフルセンタが、前記窓口センタから受け取った暗号データリストに対して、対応する公開情報を用いて順番入れ替え処理を行い、対応する復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタに返送し、

前記窓口センタが、前記第１の復号シャッフルセンタから返送されたデータリストを、第２の復号シャッフルセンタに送信し、

前記窓口センタが、最後の復号シャッフルセンタから返送されたデータリストを、復号結果リストとして出力することを特徴とする匿名復号方法。

【請求項３６】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、該暗号データリスト上の各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号方法において、

前記窓口センタが、外部から暗号データリストが入力された場合、該暗号データリストを処理順序が第１番目の復号シャッフルセンタへ転送し、

前記各復号シャッフルセンタが、前記窓口センタから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタが所有している復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタへ返送し、

前記窓口センタが、処理順序が最後の復号シャッフルセンタ以外の復号シャッフルセンタからデータリストが返送されてきた場合、処理順序が前記データリストの返送元復号シャッフルセンタの次の復号シャッフルセンタに対して前記返送されてきたデータリストを暗号データリストとして転送し、処理順序が最後の復号シャッフルセンタからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力することを特徴とする匿名復号方法。

【請求項３７】　請求項３４，３５または３６記載の匿名復号方法において、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記窓口センタに報告することを特徴とする匿名復号方法。

【請求項３８】　請求項３４，３５または３６記載の匿名復号方法において、

前記復号シャッフルセンタは、正しく順番入れ替え処理を行ったことと、正しく部分復号処理を行ったことの証明を前記処理結果のデータリストに付して前記窓口センタに報告することを特徴とする匿名復号方法。

【請求項３９】　請求項３７または３８記載の匿名復号方法において、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証することを特徴とする匿名復号方法。

【請求項４０】　請求項３７または３８記載の匿名復号方法において、

前記窓口センタは、復号シャッフルセンタが行った証明が正しいことを検証した後、前記復号シャッフルセンタから返送されてきたデータリストを暗号データリストとして、処理順序が次の復号シャッフルセンタに送信することを特徴とする匿名復号方法。

【請求項４１】　請求項３７，３８，３９または４０記載の匿名復号方法において、

前記窓口センタは、復号結果リストに、全復号シャッフルセンタから報告された証明を付して出力することを特徴とする匿名復号方法。

【請求項４２】　請求項３４，３５または３６記載の匿名復号方法において、

前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行うことを特徴とする匿名復号方法。

【請求項４３】　請求項３４，３５または３６記載の匿名復号方法において、

前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信元のデジタル署名を付与することを特徴とする匿名復号方法。

【請求項４４】　請求項３４，３５または３６記載の匿名復号方法において、

同一処理対象に対する、互いに関連する公開情報，暗号データリスト，復号シャッフルセンタが所有する復号鍵に共通のセッションＩＤを付与し、

前記窓口センタは、或るセッションＩＤに対応する暗号データリストを復号シャッフルセンタへ転送する場合および復号シャッフルセンタから返送されてきた或るセッションＩＤの付与されたデータリストを暗号データリストとして復号シャッフルセンタへ転送する場合、前記暗号データリストに前記或るセッションＩＤを付与して復号シャッフルセンタへ転送し、

前記復号シャッフルセンタは、前記窓口センタから或るセッションＩＤの付与された暗号データリストが転送されてきた場合、前記或るセッションＩＤの付与されている公開情報を用いて順番入れ替え処理を行い、前記或るセッションＩＤの付与されている復号鍵を用いて部分復号を行い、その結果のデータリストに前記或るセッショ

ンＩＤを付与して前記窓口センタに返送することを特徴とする匿名復号方法。

【請求項４５】　請求項３４，３５または３６記載の匿名復号方法において、

前記窓口センタが、セキュリティパラメータが入力されたとき、該セキュリティパラメータに基づいて共通公開情報を作成し、該作成した共通公開情報を全復号シャッフルセンタへ通知し、

前記全復号シャッフルセンタが、前記窓口センタから通知された共通公開情報に基づいて、公開鍵および復号鍵を生成し、前記生成した公開鍵を前記窓口センタへ返送し、

前記窓口センタが、前記全復号シャッフルセンタから公開鍵が返送されてきたとき、前記全復号シャッフルセンタからの公開鍵に基づいて暗号化用公開鍵を生成すると共に、該生成した暗号化用公開鍵と前記共通公開情報とを含んだ公開情報を公開することを特徴とする匿名復号方法。

【請求項４６】　請求項４５記載の匿名復号方法において、

前記復号シャッフルセンタは、公開鍵を前記窓口センタへ返送するとき、正しく前記公開鍵を生成したことの証明を付与して前記窓口センタに返送することを特徴とする匿名復号方法。

【請求項４７】　請求項４６記載の匿名復号方法において、

前記窓口センタは、公開鍵に付された証明が正しいことを検証することを特徴とする匿名復号方法。

【請求項４８】　請求項４６または４７記載の匿名復号方法において、

前記窓口センタは、公開鍵と、公開鍵に付与された証明を公開情報とともに公開することを特徴とする匿名復号方法。

【請求項４９】　請求項４５記載の匿名復号方法において、

前記窓口センタ及び前記復号シャッフルセンタは、通信時に相手認証を行うことを特徴とする匿名復号方法。

【請求項５０】　請求項４５記載の匿名復号方法において、

前記窓口センタ及び前記復号シャッフルセンタは、通信データに送信元のデジタル署名を付することを特徴とする匿名復号方法。

【請求項５１】　請求項４４記載の匿名復号方法において、

前記窓口センタは、復号シャッフルセンタに対して暗号データリストを転送する際、前記セッションＩＤに加えて、自窓口センタに付与されている窓口センタＩＤ，転送先の復号シャッフルセンタに付与されている復号シャッフルセンタＩＤ及び自窓口センタの署名も付加することを特徴とする匿名復号方法。

【請求項５２】　請求項４４記載の匿名復号方法において、

前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、前記セッションＩＤに加えて、自復号シャッフルセンタに付与されている復号シャッフルセンタＩＤ，前記窓口センタに付与されている窓口センタＩＤ及び自復号シャッフルセンタの署名も付加することを特徴とする匿名復号方法。

【請求項５３】　請求項５２記載の匿名復号方法において、

前記復号シャッフルセンタは、データリストを前記窓口センタへ返送する際、正しく順番入れ替え処理を行ったことの証明データ及び正しく部分復号処理を行ったことの証明データも付加することを特徴とする匿名復号方法。

【請求項５４】　請求項４１記載の匿名復号方法において、

前記窓口センタが出力する情報が、自窓口センタに付与されている窓口センタＩＤ，外部から入力した暗号データリスト，該暗号データリストに対する復号結果，前記暗号データリストに付与されているセッションＩＤ，全復号シャッフルセンタから返送されてきた全データ及び窓口センタの署名を含むことを特徴とする匿名復号方法。

【請求項５５】　請求項４５記載の匿名復号方法において、

前記窓口センタは、復号シャッフルセンタに対して共通公開情報およびセキュリティパラメータを通知する際、自窓口センタに付与されている窓口センタＩＤ，復号を行う全復号シャッフルセンタの復号シャッフルセンタＩＤ，セッションＩＤ及び窓口センタの署名を付加することを特徴とする匿名復号方法。

【請求項５６】　請求項４５または４６記載の匿名復号方法において、

復号シャッフルセンタは、窓口センタに返信する情報に、前記窓口センタに付与されている窓口センタＩＤ，セッションＩＤ，自復号シャッフルセンタの復号シャッフルセンタＩＤ及び自復号シャッフルセンタの署名を付加することを特徴とする匿名復号方法。

【請求項５７】　請求項４５記載の匿名復号方法において、

前記窓口センタが公開する公開情報は、自窓口センタに付与されている窓口センタＩＤ，セッションＩＤ，セキュリティパラメータ，暗号化用公開鍵，全復号シャッフルセンタの復号シャッフルセンタＩＤ及び全復号シャッフルセンタが生成した公開鍵を含むことを特徴とする匿名復号方法。

【請求項５８】　請求項３７，３８，４２または４６記載の匿名復号方法において、

復号シャッフルセンタが行った証明は、第三者により検

証できるものであることを特徴とする匿名復号方法。

【請求項５９】　請求項３４，３５または３６記載の匿名復号方法において、

前記復号シャッフルセンタは、順番入れ替え処理に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前計算したデータを用いて順番入れ替え処理を行うことを特徴とする匿名復号方法。

【請求項６０】　請求項３８記載の匿名復号方法において、

前記復号シャッフルセンタは、順番入れ替え処理が正しいことを証明する証明データの生成に用いるデータの一部分を暗号データリストを入力する前に計算し、暗号データリストを入力したとき、事前に計算したデータを用いて前記証明データを生成することを特徴とする匿名復号方法。

【請求項６１】　請求項３４乃至６０記載の何れか１つの匿名復号方法において、

投票管理センタが、各投票者から送られてくる、投票データを前記公開情報に基づいて暗号化した暗号化投票データを受け付け、その中から正当な投票者の正当な暗号化投票データを選別し、該選別した暗号化投票データを暗号データリストとして前記窓口センタに送信することを特徴とする匿名復号方法。

【請求項６２】　請求項６１記載の匿名復号方法において、

前記各投票者は、正しく投票データを暗号化したことを証明する証明データを前記投票管理センタへ送信し、

前記投票管理センタは、各投票者から送られてきた証明データを検証することを特徴とする匿名復号方法。

【請求項６３】　請求項３４乃至６０記載の何れか１つの匿名復号方法において、

入札管理センタが、各入札者から送られてくる、入札値を前記公開情報に基づいて暗号化した暗号化入札値を受け付け、その中から正当な入札者の正当な暗号化入札値を選別し、該選別した暗号化入札値を暗号化データリストとして前記窓口センタへ送信することを特徴とする匿名復号方法。

【請求項６４】　請求項６３記載の匿名復号方法において、

前記各入札者は、正しく入札値を暗号化したことを証明する証明データを前記入札管理センタへ送信し、

前記入札管理センタは、各入札者から送られてきた証明データを検証することを特徴とする匿名復号方法。

【請求項６５】　請求項３４乃至請求項６０記載の何れか１つの匿名復号方法において、

受付センタが、各アンケート回答者から送られてくる、アンケート回答を前記公開情報に基づいて暗号化した暗号化アンケート回答を受け付け、その中から正当なアンケート回答者の正当な暗号化アンケート回答を選別し、

該選別した暗号化アンケート回答を暗号化データリストとして前記窓口センタへ送信することを特徴とする匿名復号方法。

【請求項６６】　請求項６５記載の匿名復号方法において、

前記アンケート回答者は、正しくアンケート回答を暗号化したことを証明する証明データを前記受付センタへ送信し、

前記受付センタは、各アンケート回答者から送られてきた証明データを検証することを特徴とする匿名復号方法。

【請求項６７】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムを構成する窓口センタ用コンピュータ及び復号シャッフルセンタ用コンピュータの内の窓口センタ用コンピュータに、

外部から暗号データリストが入力された場合、該暗号データリストを復号シャッフルセンタ用コンピュータへ転送する処理、

前記復号シャッフルセンタ用コンピュータからデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する処理を行わせ、

前記復号シャッフルセンタ用コンピュータに、

前記窓口センタ用コンピュータから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタ用コンピュータが所有している復号鍵を用いた部分復号処理を行い、その結果のデータリストを前記窓口センタ用コンピュータへ返送する処理を行わせることを特徴とするプログラム。

【請求項６８】　指定された方法および指定された公開情報により暗号化された暗号データを複数含んだ暗号データリストを入力として、該暗号データリスト上の各暗号データの復号結果をリスト上の順番と無関係に出力する匿名復号システムを構成する窓口センタ用コンピュータ及び複数の復号シャッフルセンタ用コンピュータの内の窓口センタ用コンピュータに、

外部から暗号データリストが入力された場合、該暗号データリストを処理順序が第一番目の復号シャッフルセンタ用コンピュータへ転送する処理、

処理順序が最後の復号シャッフルセンタ用コンピュータ以外の復号シャッフルセンタ用コンピュータからデータリストが返送されてきた場合、処理順序が前記データリストの返送元復号シャッフルセンタ用コンピュータの次の復号シャッフルセンタ用コンピュータに対して前記返送されてきたデータリストを暗号データリストとして転送する処理、

処理順序が最後の復号シャッフルセンタ用コンピュータ

からデータリストが返送されてきた場合、該データリストを復号結果リストとして出力する処理を行わせ、

前記各復号シャッフルセンタ用コンピュータに、

前記窓口センタ用コンピュータから転送されてきた暗号データリストに対して、公開情報を用いた順番入れ替え処理を行うと共に自復号シャッフルセンタ用コンピュータが所有している復号鍵を用いて部分復号処理を行い、その結果のデータリストを前記窓口センタ用コンピュータへ返送する処理を行わせることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、匿名復号技術に関し、特に、暗号データとの対応を秘匿して復号結果を出力する匿名復号技術に関する。

【０００２】

【従来の技術】従来のこの種の匿名復号システムとしては、例えば、特開平08-263575 号公報に記載されているものが知られている。ここに記載されている匿名復号システムは、Mix-net 方式に基づくものであり、図１０に示すように、複数の復号シャッフルセンタ１００－１～１００－ｎと、インターネット等のネットワーク上に配置された外部からアクセス可能な電子掲示板２００とから構成されている。

【０００３】各復号シャッフルセンタ１００－１～１００－ｎは、部分復号手段１０１，シャッフル手段１０２，証明手段１０３を備えている。また、各復号シャッフルセンタ１００－１～１００－ｎは、別途定められたセキュリティパラメータに従って生成された暗号化用の公開鍵と、復号用の復号鍵とを保持している。また、図１０に示した匿名復号システムでは、各復号シャッフルセンタ１００－１～１００－ｎの公開鍵を合成したものをデータ暗号化のための暗号化用公開鍵としている。

【０００４】複数のセンダ（図示せず）が、暗号化用公開鍵を用いて暗号化した暗号データを電子掲示板２００に書き込むと、処理順序が第１番目の復号シャッフルセンタ１００－１が、上記複数のセンダが書き込んだ暗号データを暗号データリスト２０１として入力し、以下の処理を行う。

【０００５】先ず、部分復号手段１０１を用いて、暗号データリスト２０１に対する部分復号処理を行う。このとき、部分復号手段１０１は、復号シャッフルセンタ１００－１が保持している復号鍵を使用する。次に、部分復号が行われた後の暗号データリストに対して、シャッフル手段１０２を使用して順番入れ替え処理を行う。その後、証明手段１０３を用いて、部分復号処理，順番入れ替え処理が正しく行われたことを証明する証明データを生成する。そして、最後に、部分復号処理，順番入れ替え処理を行った後の暗号データリスト（データリスト）と証明データとを含むデータ２０２－１を電子掲示板２００に書き込む。

【０００６】電子掲示板２００にデータ２０２－１が書き込まれると、処理順序が第２番目の復号シャッフルセンタ１００－２が、データ２０２－１中のデータリストに対して、復号シャッフルセンタ１００－１が行った処理と同様の処理を行い、データリスト及び証明データを含むデータ２００－２を電子掲示板２００に書き込む。

【０００７】以下、同様の動作が最後の復号シャッフルセンタ１００－ｎまで行われ、電子掲示板２００に、復号結果リスト，証明データを含んだデータ２０３が書き込まれる。

【０００８】

【発明が解決しようとする課題】上述した従来の匿名復号システムは、電子掲示板を利用しているため、次のような問題があった。つまり、各復号シャッフルセンタに部分復号処理，順番入れ替え処理を行わせたり、各センダに証明データの検証を行わせるためには、各復号シャッフルセンタ，各センダから電子掲示板を自由にリードできるようにしなければならない。更に、不正行為を防止するためには、電子掲示板に対するデータの書き込みを、正当なセンダ，復号シャッフルセンタからの正当なデータのみに制限しなければならない。このように、従来の匿名復号システムは、各復号シャッフルセンタ，各センダから電子掲示板を自由にリードできるようにし、且つ、電子掲示板に対するデータの書き込みを、正当なセンダ，復号シャッフルセンタからの正当なデータのみに制限しなければならないため、管理が複雑になるという問題があった。

【０００９】また、匿名性の保護の観点から、実際の運用においては、匿名復号システムを構成する個々の復号シャッフルセンタは、すべて別々の組織によって運用されることが望ましい。しかし、別組織によって運用される場合、システムに必要な重要な各種パラメータ（利用者がメッセージを暗号化するための鍵など）を決定する初期設定作業が煩雑になるおそれがある。このため、重要なパラメータの決定経緯が不明確になるおそれがあり、ひいてはシステムの正常な運用を妨げる可能性がある。

【００１０】そこで、本発明の目的は、複雑な管理処理を不要にすると共に、初期設定作業を容易且つ確実に行えるようにすることにある。

【００１１】

【課題を解決するための手段】本発明の匿名復号システムは、１個或いは複数個の復号シャッフルセンタと、１個の窓口センタとから構成される。復号シャッフルセンタが１個の場合、窓口センタは、外部から入力された暗号データリストを復号シャッフルセンタへ転送し、復号シャッフルセンタから返送されてきたデータリスト（上記復号シャッフルセンタで暗号データリストに対して、部分復号処理，順番入れ替え処理を行ったもの）を復号

結果リストとして出力する。

【００１２】また、復号シャッフルセンタが複数個の場合は、窓口センタは、外部から入力された暗号データリストを処理順序が第１番目の復号シャッフルセンタへ転送し、上記復号シャッフルセンタからデータリストが返送されてくると、それを暗号データリストとして処理順序が第２番目の復号シャッフルセンタへ転送する。以下、窓口センタは、或る復号シャッフルセンタからデータリストが返送されてくると、それを暗号データリストとして処理順序が次の復号シャッフルセンタへ転送するという処理を繰り返し行い、処理順序が最後の復号シャッフルセンタからデータリストが返送されてくると、それを復号結果リストとして出力する。このように、本発明の匿名復号システムによれば、窓口センタと復号シャッフルセンタ間でデータをやり取りするだけで、暗号データリストを復号することが可能になり、電子掲示板を使用した従来の匿名復号システムのような複雑な管理処理が不要になる。

【００１３】また、本発明の匿名復号システムは、セキュリティパラメータが入力されたとき、窓口センタと各復号シャッフルセンタが共同して暗号化用公開鍵を含む公開情報を生成するようにしているので、初期設定作業を容易且つ確実に行うことが可能になる。

【００１４】

【発明の実施の形態】次に本発明の実施の形態について図面を参照して詳細に説明する。

【００１５】図１を参照すると、本発明の第１の実施の形態としての匿名復号システムが示されている。この匿名復号システムは、ひとつの窓口センタ１０と、複数個（ｍ個）の復号シャッフルセンタ２０－１～２０－ｍとから構成されている。

【００１６】窓口センタ１０は、コンピュータによって構成されるものであり、外部からセキュリティパラメータが入力されたとき、各復号シャッフルセンタ２０－１～２０－ｍと共同して初期設定処理を行い、暗号化用公開鍵等を含む公開情報を生成する機能や、外部から上記暗号化用公開鍵によって暗号化された暗号データを複数含む暗号データリストが入力されたとき、復号シャッフルセンタ２０－１～２０－ｍを所定の順序（例えば、外部から指示された順序）で順次使用して上記暗号データリストを復号する機能等を有する。

【００１７】このような機能を有する窓口センタ１０は、例えば、図２に示すように、窓口側初期設定手段１１と、復号制御手段１２とを備えている。

【００１８】窓口側初期設定手段１１は、外部からセキュリティパラメータが入力されたとき、各復号シャッフルセンタ２０－１～２０－ｍと共同して暗号化用公開鍵等を含む公開情報を生成し公開する機能等を有する。復号制御手段１２は、暗号データリストが入力されたとき、復号シャッフルセンタ２０－１～２０－ｍを順次使用して暗号データリストを復号し、復号結果である復号結果リストを公開する機能等を有する。

【００１９】窓口センタ１０に接続されている記録媒体Ｋ１０は、ディスク，半導体メモリ，その他の記録媒体であり、コンピュータからなる窓口センタ１０を匿名復号システムの一部として機能させるためのプログラムが記録されている。このプログラムは、コンピュータからなる窓口センタ１０によって読み取られ、その動作を制御することで、窓口センタ１０上に窓口側初期設定手段１１，復号制御手段１２を実現する。

【００２０】復号シャッフルセンタ２０－１～２０－ｍは、コンピュータによって構成されるものであり、窓口センタ１０と例えば専用回線を介して接続されている。各復号シャッフルセンタ２０－１～２０－ｍは、窓口センタ１０と共同して初期設定処理を行う機能や、窓口センタ１０から送られてきた暗号データリストに対して、順番入れ替え処理，部分復号処理を行い、その処理結果を窓口センタ１０に返送する機能等を有する。

【００２１】このような機能を有する復号シャッフルセンタ２０－ｊ（１≦ｊ≦ｍ）は、例えば、図３に示すように、シャッフル側初期設定手段２１と、シャッフル手段２２と、部分復号手段２３と、証明手段２４とを備えている。

【００２２】シャッフル側初期設定手段２１は、窓口側初期設定手段１１と共同して初期設定処理を行う機能を有する。この初期設定処理に於いて、シャッフル側初期設定手段２１は、公開鍵，復号鍵の生成を行う。シャッフル手段２２は、窓口センタ１０から送られてきた暗号データリストに対して、順番入れ替え処理を行う機能を有する。部分復号手段２３は、シャッフル手段２２が順番入れ替え処理を行った後の暗号データリストに対して、部分復号処理を行う機能を有する。証明手段２４は、シャッフル手段２２の処理が正しいことを証明する証明データを生成する機能や、部分復号手段２３の処理が正しいことを証明する証明データを生成する機能を有する。

【００２３】復号シャッフルセンタ２０－ｊに接続されている記録媒体Ｋ２０－ｊは、ディスク，半導体メモリ，その他の記録媒体であり、コンピュータからなる復号シャッフルセンタ２０－ｊを匿名復号システムの一部として機能させるためのプログラムが記録されている。このプログラムは、コンピュータからなる復号シャッフルセンタ２０－ｊによって読み取られ、その動作を制御することで、復号シャッフルセンタ２０－ｊ上にシャッフル側初期設定手段２１，シャッフル手段２２，部分復号手段２３，証明手段２４を実現する。

【００２４】次に、本実施の形態の動作について詳細に説明する。

【００２５】＜初期設定処理＞先ず、初期設定処理について説明する。

【００２６】外部からセッションＩＤの付加されたセキュリティパラメータ（ｐＬ，ｑＬ，ｔ）が入力されると、窓口センタ１０内の窓口側初期設定手段１１は、共通公開情報（ｐ，ｑ，ｇ）を生成する（図４，Ａ１）。ここで、ｐ，ｑは、エルガマル暗号のパラメータであり、或る整数ｋによりｐ＝ｋｑ＋１という関係にある２素数である。ｇは、法ｐにおける位数ｑの部分群を生成する生成元である。また、ｐＬ，ｑＬは、素数ｐ，ｑの長さであり、ｔは後述する順番入れ替え処理が正しいことを証明する証明データの生成時及び上記証明データの検証時に使用する繰り返し回数である。また、セッションＩＤは、処理対象を特定するための識別子であり、処理対象とは、例えば、県知事選挙，市議会議員選挙等である。

【００２７】その後、窓口側初期設定手段１１は、共通公開情報（ｐ，ｑ，ｇ）を含んだ公開鍵生成依頼文を作成し、それに窓口センタ１０のディジタル署名およびセッションＩＤを付して全復号シャッフルセンタ２０－１～２０－ｍへ転送する（Ａ２）。

【００２８】各復号シャッフルセンタ２０－１～２０－ｍ内のシャッフル側初期設定手段２１は、公開鍵生成依頼文に付されているディジタル署名を検証することにより、相手認証を行う（Ａ３）。そして、署名が正しくなければ、例えば処理終了とする。これに対して、署名が正しければ、共通公開情報（ｐ，ｑ，ｇ）の正当性を確認する。すなわち、（ｐ，ｑ，ｇ）が第[００２６]段落に記載されている関係を満たすかどうか調べる。正当性を確認できなければ、例えば処理終了とする。これに対して正当性を確認できれば、共通公開情報（ｐ，ｑ，ｇ）に基づいて、公開鍵および復号鍵（秘密鍵）を生成し、それらを自復号シャッフルセンタ内に、セッションＩＤと対応付けて保持する（Ａ４）。例えば、処理順序が第ｊ番目の復号シャッフルセンタ２０－ｊにおいては、無作為に$x_j \bmod q$を選び、それを復号鍵とする。また、自復号シャッフルセンタ２０－ｊの公開鍵y_jを

$$y_j = g^{x_j} \bmod p$$

により生成する。

【００２９】その後、各復号シャッフルセンタ２０－１～２０－ｍ内のシャッフル側初期設定手段２１は、ステップＡ４で生成した公開鍵に対して復号鍵を知っていることの証明データを生成する（Ａ５）。例えば、処理順序が第ｊ番目の復号シャッフルセンタ２０－ｊ内のシャッフル側初期設定手段２１では、公開鍵y_jに対して復号鍵x_jを知っていることの証明データy'_j，r_jを

$$\begin{aligned} y'_j &= g^{\beta_j} \bmod p \\ c_j &= Hash(p, q, g, y_j, y'_j) \\ r_j &= c_j x_j + \beta_j \bmod q \end{aligned}$$

により生成する。ここで、Ｈａｓｈは安全なハッシュ関数、β_jは乱数である。

【００３０】ステップＡ５の処理が終了すると、各復号シャッフルセンタ２０－１～２０－ｍ内のシャッフル側初期設定手段２１は、ステップＡ４で生成した公開鍵及びステップＡ５で生成した証明データを含む公開鍵登録依頼文を作成し、それに自復号シャッフルセンタのディジタル署名及びセッションＩＤを付して窓口センタ１０へ返送する（Ａ６）。

【００３１】窓口センタ１０内の窓口側初期設定手段１１は、各復号シャッフルセンタ２０－１～２０－ｍから返送されてきた公開鍵登録依頼文に付されているディジタル署名を検証することにより相手認証を行い（Ａ７）、更に、各復号シャッフルセンタ２０－１～２０－ｍから返送されてきた公開鍵の正当性を

$$\begin{aligned} c_j &= Hash(p, q, g, y_j, y'_j) \\ g^{r_j} y_j{}^{-c_j} &= y'_j \bmod p \\ y_j{}^q &= 1 \bmod p \\ y_j &\neq 1 \bmod p \end{aligned}$$

により検証する（Ａ８）。

【００３２】そして、復号シャッフルセンタ２０－１～２０－ｍから返送されてきた全ての公開鍵登録依頼文が、ステップＡ７，Ａ８の検証を通った場合は、各復号シャッフルセンタ２０－１～２０－ｍから返送されてきた公開鍵y_1～y_mを、

$$Y = \prod_{j=1}^{m} y_j \bmod p$$

により合成し、システム利用者がデータを暗号化する際に使用する暗号化用公開鍵Ｙを生成する（Ａ９）。

【００３３】その後、窓口側初期設定手段１１は、暗号化用公開鍵Ｙ，各復号シャッフルセンタ２０－１～２０－ｍの公開鍵y_1～y_m，共通公開情報（ｐ，ｑ，ｇ）及び各復号シャッフルセンタ２０－１～２０－ｍの復号シャッフルセンタＩＤ（どのような組織が復号を担当しているのかをシステム利用者に知らせるため）を含む公開情報を生成し、この公開情報をセッションＩＤと対応付けて公開する（Ａ１０）。以上が初期設定処理である。

【００３４】次に、復号処理について説明する。

【００３５】窓口センタ１０内の復号制御手段１２には、外部からｎ個の暗号データを含んだ暗号データリスト$\{(G_i, M_i)\}_{(i=1,2,\cdots,n)}$が入力される。この暗号データリストには、それがどの処理対象に関連するものであるのかを特定するためのセッションＩＤが付与されている。

【００３６】暗号データ（G_i，M_i）は、データm_iに対応する暗号データであり、

$$(G_i, M_i) = (g^{r_i}, m_i Y^{r_i}) \bmod p$$

により得られたものである。ここで、データm_iは、位数がｑになるように選ばれているものとする。また、r_iは、データm_iに対して任意に選んだ乱数である。

【００３７】窓口センタ１０内の復号制御手段１２は、暗号データリスト｛（G_i，M_i）｝$_{(i=1,2,\cdots,n)}$が入力されると、G_i，M_iの位数がｑであることを全てのｉについて確認したのち、それに窓口センタ１０のディジタル署名，セッションＩＤを付して処理順序が第１番目の復号シャッフルセンタ２０－１に転送する（図５，Ｂ１，Ｂ２）。尚、処理順序が第ｊ番目の復号シャッフルセンタ２０－ｊへ転送する暗号データリストは、｛（$G^{(j)}_i$，$M^{(j)}_i$）｝$_{(i=1,2,\cdots,n)}$と記すものとする。

【００３８】復号シャッフルセンタ２０－１は、暗号データリスト｛（$G^{(1)}_i$，$M^{(1)}_i$）｝$_{(i=1,2,\cdots,n)}$に付されているディジタル署名を検証することにより相手認証を行う（図６，Ｃ１）。そして、ディジタル署名が正しいものであれば、シャッフル手段２２，部分復号手段２３を用いて上記暗号データリストに対して順番入れ替え処理，部分復号処理を行い、処理結果であるデータリストを得る（Ｃ２，Ｃ３）。尚、順番入れ替え処理，部分復号処理については、後で詳細に説明する。その後、証明手段２４を用いてシャッフル手段２２，部分復号手段２３が行った処理が正しいことを示す証明データを生成し（Ｃ４）、データリスト，証明データにディジタル署名およびセッションＩＤを付して窓口センタ１０へ返送する（Ｃ５）。ここで、証明データは、データリストに付加して窓口センタ１０へ返送しても良いし、先にデータリストだけを返送し、後から証明データを個別で返送するようにしても良い。尚、証明データの生成方法については、後で詳細に説明する。

【００３９】窓口センタ１０内の復号制御手段１２は、復号シャッフルセンタ２０－１からディジタル署名，セッションＩＤの付されたデータリスト，証明データが返送されてくると、ディジタル署名に基づいて、相手認証を行うと共に、証明データを検証する（図５，Ｂ３）。尚、証明データの検証方法については、後で詳細に説明する。そして、ディジタル署名，証明データが正しいものである場合は、処理順序が第２番目の復号シャッフルセンタ２０－２に、処理順序が第１番目の復号シャッフルセンタ２０－１から返送されてきたデータリストを暗号データリストとして転送する（Ｂ４～Ｂ６）。その際、復号制御手段１２は、暗号データリストに、セッションＩＤを付加する。

【００４０】復号シャッフルセンタ２０－２でも、復号シャッフルセンタ２０－１と同様の処理が行われ（図６，Ｃ１～Ｃ５）、窓口センタ１０にディジタル署名，セッションＩＤの付されたデータリスト，証明データが返送される。

【００４１】これにより、窓口センタ１０内の復号制御手段１２は、前述した処理と同様の処理を行う（図５，Ｂ３～Ｂ６）。以上の処理が繰り返し行われ、処理順序が最後の復号シャッフルセンタ２０－ｍからディジタル署名，セッションＩＤの付されたデータリスト，証明データが返却されると、復号制御手段２０は、上記データリストを復号結果リストとして公開する（Ｂ７）。その際、各復号シャッフルセンタ２０－１～２０－ｍから送られてきた各証明データ，セッションＩＤ，窓口センタ１０の窓口センタＩＤ，復号シャッフルセンタ２０－１～２０－ｍの復号シャッフルセンタＩＤも公開する。

【００４２】以下に、シャッフル手段２２が行う順番入れ替え処理，部分復号手段２３が行う部分復号処理，証明手段２４が行う証明データ生成処理，復号制御手段１２が行う検証処理について詳しく説明する。

【００４３】＜順番入れ替え処理＞処理順序が第ｊ番目の復号シャッフルセンタ２０－ｊ内のシャッフル手段２２が行う順番入れ替え処理について説明する。順番入れ替え処理は、以下に述べるシャッフル処理と再暗号処理とからなる。

【００４４】シャッフル手段２２は、先ず、シャッフル処理を行う。シャッフル処理においては、窓口センタ１０から送られてきた暗号データリスト｛（$G^{(j)}_i$，$M^{(j)}_i$）｝$_{(i=1,2,\cdots,n)}$中の暗号データ（$G^{(j)}_i$，$M^{(j)}_i$）$_{(i=1,2,\cdots,n)}$に対して、ランダムに置換写像$\pi^{(j)}$を決定し、それに基づいて（$G^{(j)}_i$，$M^{(j)}_i$）$_{(i=1,2,\cdots,n)}$の順番を入れ替え、新たに、

$$\{(\bar{G}_i^{(j)}, \bar{M}_i^{(j)})\}_{(i=1,2,\ldots,n)}$$

を得る。以上がシャッフル処理である。このとき、

$$\{(\bar{G}_i^{(j)}, \bar{M}_i^{(j)})\} = \{(G^{(j)}_{\pi^{(j)}(i)}, M^{(j)}_{\pi^{(j)}(i)})\}(i = 1, 2, \ldots, n)$$

が成り立っている。

【００４５】シャッフル処理が終了すると、再暗号処理を行う。ここで、再暗号とは、暗号化されたデータの内容を変えずに暗号データの「見かけ」を変えることである。単に位置を変えただけでは、暗号データのビットパターンから暗号データを追跡することが可能であるため、再暗号処理が必要になる。

【００４６】そこで、処理順序が第ｊ番目の復号シャッフルセンタ２０－ｊ内のシャッフル手段２２は、自復号シャッフルセンタ以降の復号シャッフルセンタの公開鍵を合成して、

$$Y_j = \prod_{\ell=j}^{m} y_\ell \bmod p$$

を求める。そして、シャッフル処理された

$$\{(\bar{G}_i^{(j)}, \bar{M}_i^{(j)})\}_{(i=1,2,\ldots,n)}$$

に対して、乱数$s^{(j)}_i$ mod ｑを発生させて、

$$G'^{(j)}_i = \bar{G}^{(j)}_i \cdot g^{s^{(j)}_i} \bmod p$$
$$M'^{(j)}_i = \bar{M}^{(j)}_i \cdot Y_j^{s^{(j)}_i} \bmod p$$

により、｛（G'$^{(j)}_i$，M'$^{(j)}_i$）｝$_{(i=1,2,\cdots,n)}$を求める。

【００４７】尚、Y_iや、乱数s$^{(j)}_i$の発生、および

$$g^{s^{(j)}_i},\ Y_j^{s^{(j)}_i}$$

の計算は、暗号データリストを受け取る前に事前計算しておくことができる。事前計算した値を保存しておけば、各データ成分に対して、この再暗号処理は、１回の乗算のみで実現できる。

【００４８】＜部分復号処理＞次に、復号シャッフルセンタ２０－ｊ内の部分復号手段２３が行う部分復号処理について説明する。

【００４９】部分復号手段２３は、シャッフル手段２２が順番入れ替え処理を行った｛（G'$^{(j)}_i$，M'$^{(j)}_i$）｝$_{(i=1,2,\cdots,n)}$に対して、自復号シャッフルセンタ２０－ｊが所有している復号鍵x_i（暗号データリストに付されているセッションＩＤに対応する復号鍵）を用いて、

$$M''^{(j)}_i = M'^{(j)}_i / (G'^{(j)}_i)^{x_j} \bmod p$$
$$G''^{(j)}_i = G'^{(j)}_i$$

を計算する。そして、

$$(G''^{(j)}_i, M''^{(j)}_i)_{(i=1,2,\cdots,n)}$$

をデータリストとして窓口センタ１０へ返送する。

＊【００５０】＜証明データ生成処理＞次に、証明手段２４が行う証明データ生成処理について説明する。尚、以下の説明においては、復号シャッフルセンタを特定する（ｊ）の表記を省略する。

【００５１】先ず、シャッフル手段２２がデータリスト｛（G'$_i$，M'$_i$）｝$_{(i=1,2,\cdots,n)}$に対して、置換写像πを用いてシャッフル処理を行い、公開鍵情報（ｐ，ｑ，ｇ，Y_i）と乱数列｛s_i｝$_{(i=1,2,\cdots,n)}$を用いて｛（G$^{(j)}_i$，M$^{(j)}_i$）｝$_{(i=1,2,\cdots,n)}$を生成したことを、置換写像πと乱数列｛s_i｝を秘密にして証明する証明データの生成方法について説明する。尚、以下の説明において、ｔはセキュリティパラメータ（繰り返し回数）である。

【００５２】１．ｔ個のランダムな置換写像π'$_u$と、ｔ×ｎ個の乱数｛s'$_{(u,v)}$｝を発生させ、

$$A_{u,v} = G_{\pi'_u(v)} \cdot g^{s'_{(u,v)}} \bmod p$$
$$B_{u,v} = M_{\pi'_u(v)} \cdot Y_j^{s'_{(u,v)}} \bmod p$$

をｕ＝１，２，…，ｔ、ｖ＝１，２，…，ｎに関して計算する。２．

$$c = Hash(p||q||g||Y_j||\{(G_i, M_i)\}_{(i=1,\cdots,n)}||$$
$$\{(G'_i, M'_i)\}_{(i=1,\cdots,n)}||$$
$$\{(A_{(u,v)}, B_{(u,v)})\}_{(u=1,\cdots,t,v=1,\cdots,n)})$$

を計算する。ここで、||は連結を示す。３．ｃのｕ番目（ｕ＝１，２，…，ｔ）のビットをｃ〔ｕ〕とすると、

- $c[u]=0$のとき、$\alpha_u = \pi'_u$及び$\beta_{(u,v)} = s'_{(u,v)}$とおく。
- $c[u]=1$のとき、$\alpha_u = \pi^{-1} \circ \pi'_u$及び$\beta_{(u,v)} = s'_{(u,v)} - s_{(\pi^{-1}\circ\pi'_v(u))}$とおく。

とおく。証明データは、｛（G'$^{(j)}_i$，M'$^{(j)}_i$）$_{(i=1,2,\cdots,n)}$｝，｛A$_{(u,v)}$，B$_{(u,v)}$｝，｛α_u｝，｛$\beta_{(u,v)}$｝となる。

【００５３】尚、置換写像π'$_u$や乱数｛s'$_{(u,v)}$｝の発生および

$$g^{s'_{(u,v)}},\ Y_j^{s'_{(u,v)}}$$

の計算は、暗号データリストを受け取る前に事前計算しておくことができる。事前計算をした値を保存しておけば、処理時間を短縮することが可能になる。

【００５４】次に、上記した｛（G'$_i$，M'$_i$）｝$_{(i=1,2,\cdots,n)}$に対して、自分の公開鍵ｙに対する秘密鍵ｘを用いて正しく計算した｛（G"$_i$，M"$_i$）$_{(i=1,2,\cdots,n)}$｝を窓口センタ１０に送ったことを秘密鍵ｘを漏らさずに証明する証明データの生成方法について説明する。

【００５５】１．乱数ｒ mod ｑを生成する。

２．

$$c = Hash(p||q||g||y||\{G'_i\}_{(i=1,\cdots,n)}||$$
$$\{(M'_i/M''_i)\}_{(i=1,\cdots,n)}||g^r||\{G'^r_i\}_{(i=1,\cdots,n)})$$

とおく。

３．$\alpha = r - cx \bmod q$とおく。

以上のようにして求めたｃ，αが証明データとなる。

【００５６】＜検証処理＞次に、復号制御手段１２が行う検証処理について説明する。先ず、シャッフル手段２２の処理が正しいことを証明する証明データの検証について説明する。

【００５７】１．公開された情報及び証明データから

$$c = Hash(p||q||g||Y_j||\{(G_i, M_i)\}_{(i=1,\cdots,n)}||$$
$$\{(G'_i, M'_i)\}_{(i=1,\cdots,n)}||$$
$$\{(A_{(u,v)}, B_{(u,v)})\}_{(u=1,\cdots,t,v=1,\cdots,n)})$$

を計算する。

２．ｃのｕ番目（ｕ＝１，２，…，ｔ）のビットをｃ〔ｕ〕とすると、・ｃ〔ｕ〕＝０のとき、

$$A_{u,v} = G_{\alpha_u(v)} \cdot g^{\beta_{(u,v)}} \bmod p$$
$$B_{u,v} = M_{\alpha_u(v)} \cdot Y_j^{\beta_{(u,v)}} \bmod p$$

が成り立つことを確認する。

・ｃ〔ｕ〕＝１のとき、

$$A_{u,v} = G'_{\alpha_u(v)} \cdot g^{\beta_{(u,v)}} \bmod p$$
$$B_{u,v} = M'_{\alpha_u(v)} \cdot Y_j^{\beta_{(u,v)}} \bmod p$$

が成り立つことを確認する。

３．G'_i, M'_iの位数がｑであることを確認する。全てが確認できれば、証明データは正しいとみなす。

【００５８】次に、部分復号手段２３が行った処理が正しいことを証明する証明データの検証について説明する。

【００５９】１．全てのｉについて$G'_i = G''_i$であることを確認する。

【００６０】２．

$$c = Hash(p||q||g||y||\{G'_i\}_{(i=1,\cdots,n)}||$$
$$\{(M'_i/M''_i)\}_{(i=1,\cdots,n)}||g^{\alpha} \cdot y^{c}||$$
$$\{G'^{\alpha}_i \cdot (M'_i/M''_i)^{c}\}_{(i=1,\cdots,n)})$$

が成り立つことを確認する。

【００６１】３．全てのｉについて$M''^{q}_i = 1 \bmod p$であることを確認する。全てが確認できれば、証明データは正しいとみなす。実際には、シャッフル証明と復号証明は一度に行われる。従って、復号結果として与えられている$\{G''_i\}_{(i=1,2,\cdots,n)}$に対して$G'_i = G''_i$となるはずの$\{G'_i\}_{(i=1,2,\cdots,n)}$を送る必要はない。従って、実装では、シャッフル証明時に$\{M'_i\}_{(i=1,2,\cdots,n)}$のみを送るようにする。

【００６２】尚、以上の動作説明では説明を省略したが、窓口センタと復号シャッフルセンタとでデータをやり取りする場合には、データに転送先の窓口センタ，復号シャッフルセンタのＩＤ及び転送元の窓口センタ，復号シャッフルセンタのＩＤを付加するものとする。例えば、窓口センタ１０から復号シャッフルセンタ２０－１へデータを転送する場合には、復号シャッフルセンタ２０－１，窓口センタのＩＤをそれぞれ転送先，転送元として付加する。また、例えば、窓口センタ１０から全ての復号シャッフルセンタ２０－１～２０－ｍへデータを転送する場合には、全復号シャッフルセンタ２０－１～２０－ｍのＩＤ，窓口センタ１０のＩＤをそれぞれ転送先，転送元として付加する。

【００６３】次に、図７を参照して本発明の第２の実施の形態について説明する。本実施の形態は、無記名電子投票を行う際に利用すると好適なものであり、図１に示した匿名復号システムが備えている構成に加え、投票管理センタ３０が追加されている。

【００６４】投票管理センタ３０には、有権者名簿と、セキュリティパラメータと、選挙の投票期間と、セッションＩＤとが入力される。投票管理センタ３０は、上記セキュリティパラメータに上記セッションＩＤを付加し、窓口センタ１０へ転送する。

【００６５】窓口センタ１０は、投票管理センタ３０からセッションＩＤの付与されたセキュリティパラメータが送られてくると、各復号シャッフルセンタ２０－１～２０－ｍと共同して前述した初期設定処理（図４参照）を行い、得られた公開情報（公開鍵Ｙ，共通公開情報ｐ，ｑ，ｇ等を含む）を公開する。投票管理センタ３０は、その公開情報がセキュリティパラメータに従っていて正当なものであることを確認し、各投票者に通知する。

【００６６】投票期間が始まると投票者は、自分の投票データを公開情報を基に暗号化し、投票者のディジタル署名を付加して投票管理センタ３０に送付する。ここで、第ｉ（＝１，２，…，ｎ）番目の投票者は、公開された公開鍵Ｙ及び共通公開情報（ｐ，ｑ，ｇ）を用いて投票内容m_iを以下のように暗号化する。尚、ここで、投票内容は位数がｑになるように選ばれているものとする。

【００６７】先ず、投票者は、任意の乱数$r_i \bmod q$を選ぶ。次に、

$$(G_i, M_i) = (g^{r_i}, m_i Y^{r_i}) \bmod p$$

により得られた(G_i, M_i)を暗号投票データとする。この暗号投票データに自身のディジタル署名を付して投票センタ３０へ送付する。

【００６８】ここで、投票者が正しくm_iを知って暗号投票データを作成したことの証明を施すことができる。例えば、第ｉ番目の投票者は、乱数γを発生させ、

$$\alpha_i = g^{\gamma_i} \bmod p$$
$$c_i = Hash(p, q, g, G_i, \alpha_i)$$
$$t_i = c_i r_i + \gamma_i \bmod q$$

により、証明データα，t_iを生成する。この証明は、

$$c_i = Hash(p, q, g, G_i, \alpha_i)$$
$$g^{t_i} G_i^{-c_i} = \alpha_i \bmod p$$

により検証することができる。

【００６９】或いは、第ｉ番目の投票者は、乱数γを発生させ、

$$\alpha_i = g^{\gamma_i} \bmod p$$
$$c_i = Hash(p, q, g, G_i, \alpha_i)$$
$$t_i = \gamma_i - c_i r_i \bmod q$$

により、証明データα，t_iを生成しても良い。この証

明は、

$$c_i = Hash(p, q, g, G_i, \alpha_i)$$
$$g^{t_i} G_i^{c_i} = \alpha_i \bmod p$$

により検証することができる。

【００７０】投票管理センタ３０は、署名を検証し、有権者名簿をもとに投票者の投票権を確認し、二重投票をチェックした後、投票を受け付ける。尚、証明データが付加されている場合は、更に、証明データを検証した後、投票を受け付ける。投票期間が終わると投票の受け付けを終了し、受け付けた暗号投票データを暗号データリストとして匿名復号システムの窓口センタ１０にディジタル署名付きで送信する。窓口センタ１０は、暗号データリストを受け取ると、前述の復号処理によってデータリストを復号し、復号結果や証明データを投票管理センタ３０に返送する。

【００７１】投票管理センタ３０は、受け取った復号結果を復号後の投票データとして集計し、発表する。

【００７２】次に、図８を参照して本発明の第３の実施の形態について説明する。本実施の形態は、匿名電子入札を行う際に利用すると好適なものであり、図１に示した匿名復号システムが備えている構成に加え、入札管理センタ４０が追加されている。

【００７３】入札管理センタ４０には、入札者名簿と、セキュリティパラメータと、入札期間と、セッションＩＤとが入力される。入札管理センタ４０は、上記セキュリティパラメータに上記セッションＩＤを付加し、窓口センタ１０へ転送する。

【００７４】窓口センタ１０は、入札管理センタ４０からセッションＩＤの付与されたセキュリティパラメータが送られてくると、各復号シャッフルセンタ２０－１～２０－ｍと共同して前述した初期設定処理（図４参照）を行い、得られた公開情報（公開鍵Ｙ，共通公開情報ｐ，ｑ，ｇ等を含む）を公開する。入札管理センタ４０は、その公開情報がセキュリティパラメータに従っていて正当なものであることを確認し、各入札者に通知する。

【００７５】入札期間が始まると入札者は、自分の入札値を公開情報を基に暗号化し、入札者のディジタル署名を付加して入札管理センタ４０に送付する。その際、自分の入札値を知っていることを証明する証明データ（第２の実施の形態で説明した証明データと同様の証明データ）を送付するようにしても良い。

【００７６】入札管理センタ４０は、署名を検証し、入札者名簿をもとに入札者の入札権を確認し、二重の入札がないかをチェックした後、入札を受け付ける。尚、証明データも送付される場合には、証明データを検証した後、入札を受け付ける。入札期間が終わると入札の受け付けを終了し、受け付けた暗号入札値を暗号データリストとして匿名復号システムの窓口センタ１０に送信する。窓口センタ１０は、暗号データリストを受け取ると、前述の復号処理によってデータリストを復号し、復号結果や証明データを入札管理センタ４０に返送する。

【００７７】入札管理センタ４０は、受け取った復号結果を復号後の入札値として発表する。

【００７８】次に、図９を参照して本発明の第４の実施の形態について説明する。本実施の形態は、匿名電子アンケートを行う際に利用すると好適なものであり、図１に示した匿名復号システムが備えている構成に加え、受付センタ５０が追加されている。

【００７９】受付センタ５０には、回答者名簿と、セキュリティパラメータと、アンケート期間と、セッションＩＤとが入力される。受付センタ５０は、上記セキュリティパラメータに上記セッションＩＤを付加し、窓口センタ１０へ転送する。

【００８０】窓口センタ１０は、受付センタ５０からセッションＩＤの付与されたセキュリティパラメータが送られてくると、各復号シャッフルセンタ２０－１～２０－ｍと共同して前述した初期設定処理（図４参照）を行い、得られた公開情報（公開鍵Ｙ，共通公開情報ｐ，ｑ，ｇ等を含む）を公開する。受付センタ５０は、その公開情報がセキュリティパラメータに従っていて正当なものであることを確認し、各アンケート回答者に通知する。

【００８１】アンケート期間が始まるとアンケート回答者は、自分のアンケート回答を公開情報を基に暗号化し、アンケート回答者のディジタル署名を付加して受付センタ５０に送付する。その際、自分のアンケート回答を知っていることを証明する証明データ（第２の実施の形態で説明した証明データと同様の証明データ）を送付するようにしても良い。

【００８２】受付センタ５０は、署名を検証し、回答者名簿をもとに回答者の回答権を確認し、二重回答がないかをチェックした後、アンケート回答を受け付ける。尚、証明データも送付される場合には、証明データを検証した後、アンケート回答を受け付ける。アンケート期間が終わるとアンケート回答の受け付けを終了し、受け付けた暗号アンケート回答を暗号データリストとして匿名復号システムの窓口センタ１０に送信する。窓口センタ１０は、暗号データリストを受け取ると、前述の復号処理によってデータリストを復号し、復号結果や証明データを受付センタ５０に返送する。

【００８３】受付センタ５０は、受け取った復号結果を復号後のアンケート回答として発表する。

【００８４】なお、本実施例で述べた以外にも、センタ或いは第三者が、公開されている情報やデータの正当性を適宜検証することが考えられる。また、証明方法に関する数式は一例であり、式を変更して同様の効果がえられることは同業者は容易に想定できることである。

【００８５】

27

【発明の効果】以上説明したように、本発明によれば、窓口センタと復号シャッフルセンタとの間でデータをやり取りするだけで暗号データリストを復号することが可能になり、電子掲示板を用いた従来の匿名復号システムのような複雑な管理処理が不要になるという効果がある。

【００８６】また、本発明では、外部から入力されたセキュリティパラメータに基づいて、窓口センタと復号シャッフルセンタが共同して暗号化用公開鍵を含む公開情報を生成するので、初期設定操作を容易且つ確実に行うことが可能になる効果がある。

【００８７】また、復号鍵という重要な秘密を管理する復号シャッフルセンタが、不特定多数からアクセスされる電子掲示板と直接接続する必要が生じないので、セキュリティ面の効果が顕著である。更に、復号シャッフルセンタの構成を、復号鍵に関わる処理と窓口センタとの通信機能のみに集約できるので、コンパクトに実現できるという効果がある。また、窓口センタと復号シャッフルセンタで、セッション管理機能と復号鍵管理機能をそれぞれ分担したので、１度きりの匿名復号のみならず、複数回の匿名復号処理や、電子投票、電子入札、電子アンケートなど、すべて高いセキュリティでサービスを実現できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の構成例を示すブロック図である。

【図２】窓口センタ１０の構成例を示すブロック図である。

【図３】復号シャッフルセンタ２０－ｊの構成例を示すブロック図である。

【図４】初期設定時の処理例を示す流れ図である。

【図５】復号制御手段１２の処理例を示す流れ図である。

28

＊【図６】復号シャッフルセンタ２０－１～２０－ｍの処理例を示す流れ図である。

【図７】本発明の第２の実施の形態の構成例を示すブロック図である。

【図８】本発明の第３の実施の形態の構成例を示すブロック図である。

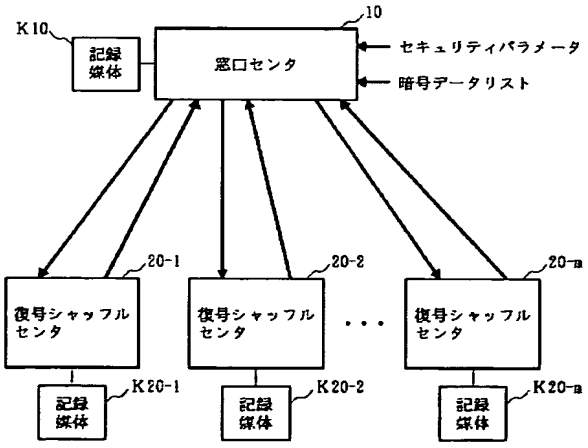
【図９】本発明の第４の実施の形態の構成例を示すブロック図である。

【図１０】従来の技術を説明するためのブロック図である。

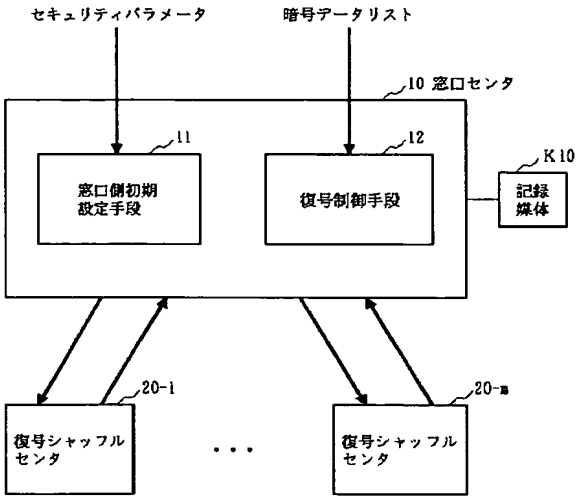
【符号の説明】

１０…窓口センタ
１１…窓口側初期設定手段
１２…復号制御手段
Ｋ１０…記録媒体
２０－１～２０－ｍ…復号シャッフルセンタ
２１…シャッフル側初期設定手段
２２…シャッフル手段
２３…部分復号手段
２４…証明手段
Ｋ２０－１～Ｋ２０－ｍ…記録媒体
３０…投票管理センタ
４０…入札管理センタ
５０…受付センタ
１００－１～１００－ｎ…復号シャッフルセンタ
１０１…部分復号手段
１０２…シャッフル手段
１０３…証明手段
２００…電子掲示板
２０１…暗号データリスト
２０２－１，２０２－２…処理された暗号データリスト，証明データを含むデータ
２０３…復号結果リスト，証明データを含むデータ

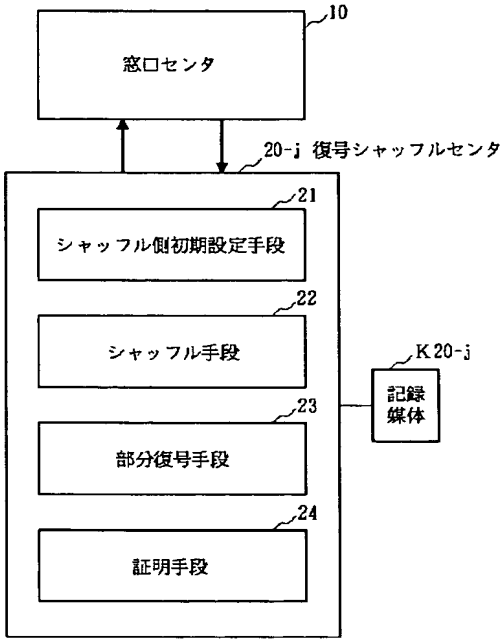
【図１】



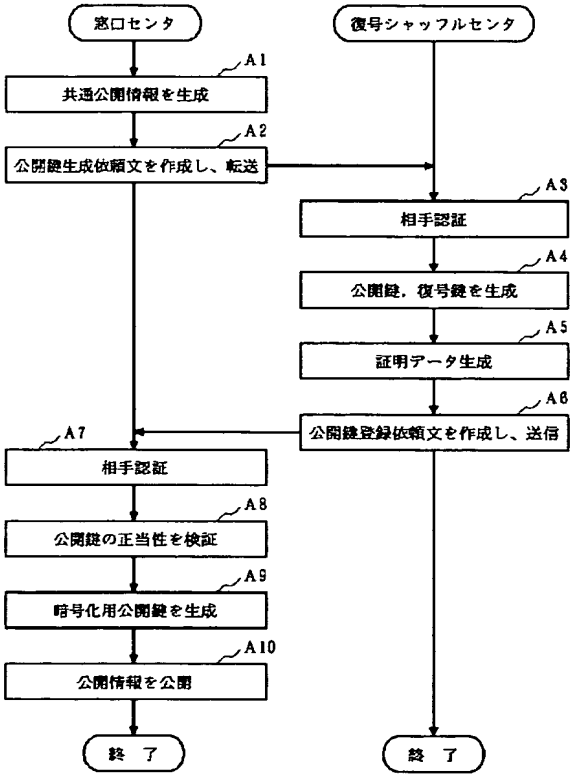
【図２】


セキュリティパラメータ
暗号データリスト
10 窓口センタ
11
窓口側初期設定手段
12
復号制御手段
K10
記録媒体
20-1
復号シャッフルセンタ
20-m
復号シャッフルセンタ

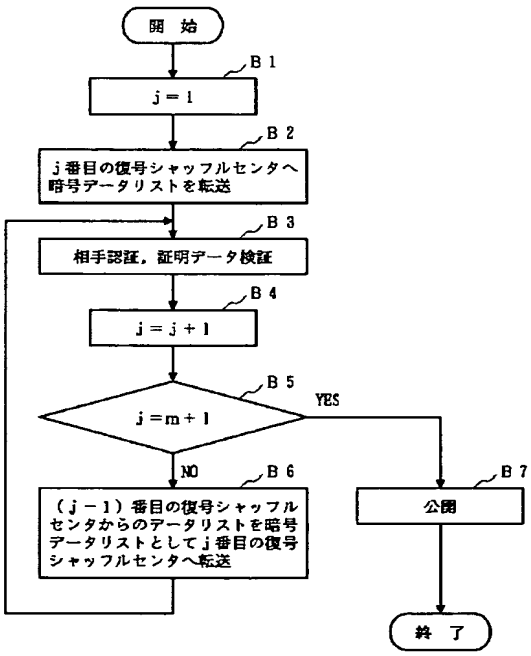
【図３】


10
窓口センタ
20-j 復号シャッフルセンタ
21
シャッフル側初期設定手段
22
シャッフル手段
23
部分復号手段
24
証明手段
K20-j
記録媒体

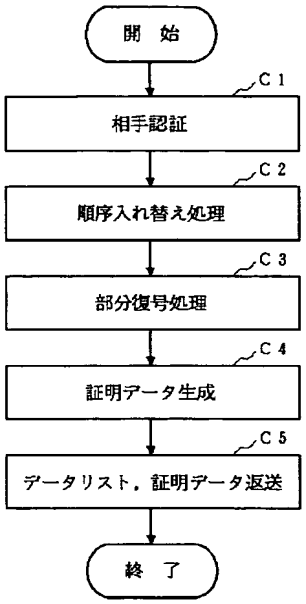
【図４】


窓口センタ
復号シャッフルセンタ
A1
共通公開情報を生成
A2
公開鍵生成依頼文を作成し、転送
A3
相手認証
A4
公開鍵，復号鍵を生成
A5
証明データ生成
A6
公開鍵登録依頼文を作成し、送信
A7
相手認証
A8
公開鍵の正当性を検証
A9
暗号化用公開鍵を生成
A10
公開情報を公開
終 了
終 了

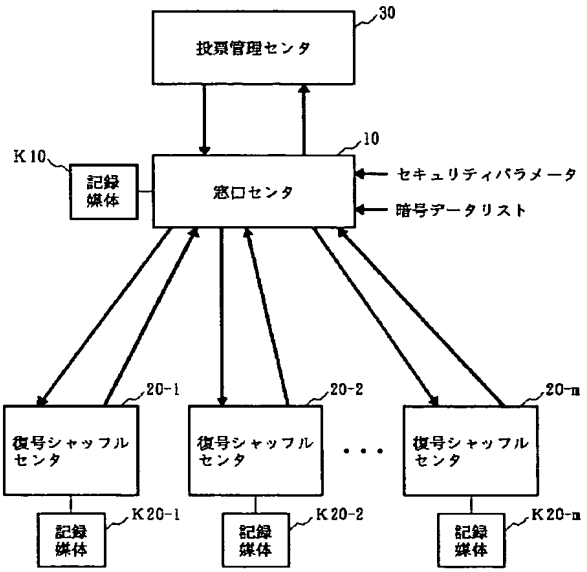
【図５】


開 始
B1
j＝1
B2
j番目の復号シャッフルセンタへ暗号データリストを転送
B3
相手認証，証明データ検証
B4
j＝j＋1
B5
j＝m＋1
YES
NO
B6
（j－1）番目の復号シャッフルセンタからのデータリストを暗号データリストとしてj番目の復号シャッフルセンタへ転送
B7
公開
終 了

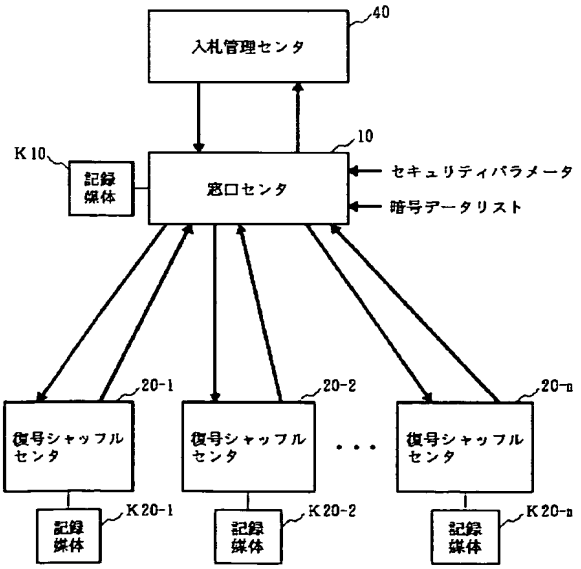
【図６】


開　始
C 1
相手認証
C 2
順序入れ替え処理
C 3
部分復号処理
C 4
証明データ生成
C 5
データリスト，証明データ返送
終　了

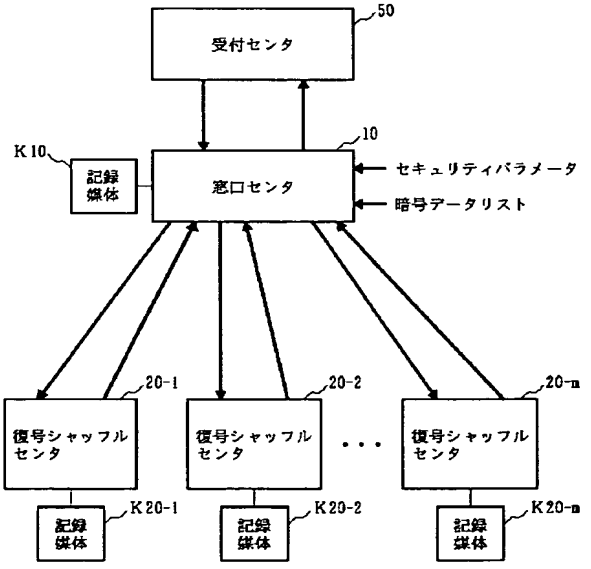
【図７】


投票管理センタ
30
K10
記録媒体
10
窓口センタ
セキュリティパラメータ
暗号データリスト
20-1
20-2
20-n
復号シャッフルセンタ
復号シャッフルセンタ
復号シャッフルセンタ
記録媒体
K20-1
記録媒体
K20-2
記録媒体
K20-n

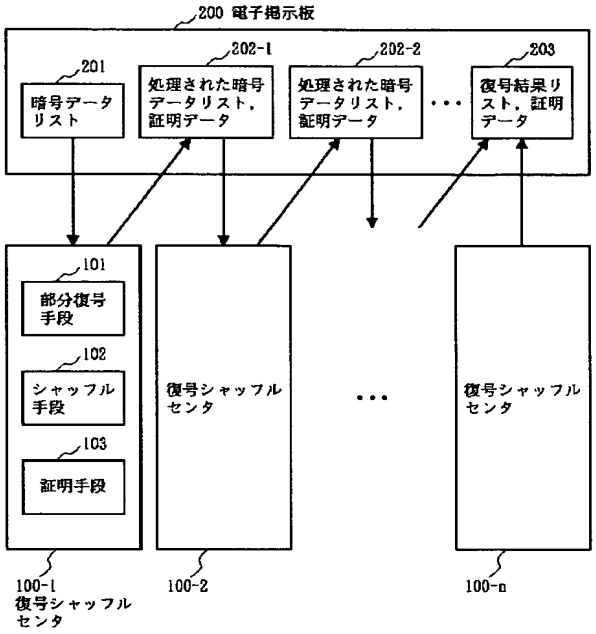
【図８】


入札管理センタ
40
K10
記録媒体
10
窓口センタ
セキュリティパラメータ
暗号データリスト
20-1
20-2
20-n
復号シャッフルセンタ
復号シャッフルセンタ
復号シャッフルセンタ
記録媒体
K20-1
記録媒体
K20-2
記録媒体
K20-n

【図９】


受付センタ
50
K10
記録媒体
10
窓口センタ
セキュリティパラメータ
暗号データリスト
20-1
20-2
20-n
復号シャッフルセンタ
復号シャッフルセンタ
復号シャッフルセンタ
記録媒体
K20-1
記録媒体
K20-2
記録媒体
K20-n

【図１０】


200 電子掲示板
201
暗号データリスト
202-1
処理された暗号データリスト，証明データ
202-2
処理された暗号データリスト，証明データ
203
復号結果リスト，証明データ
101
部分復号手段
102
シャッフル手段
103
証明手段
復号シャッフルセンタ
復号シャッフルセンタ
100-1
復号シャッフルセンタ
100-2
100-n